***What is claimed is:***

1. An end to end real-time encrypting module of a mobile commerce WAP data transmission section, wherein the uppermost layer of the wireless application environment (WAE) is used as a developing platform and executing environment and is suitable for various communication networks, such as GSM, PDC, CDPD, CDMA, TDMA, PHS, DECT, GPRS and third generation mobile phone (3G); an information encryption code security system matching the public key infrastructure is installed in a WML server end of a current mobile server of a wireless service provider; and the system includes a handset software encryption and decryption module, a cipher server, and a key management.

2. The end to end real-time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1, wherein when an user registers into the WML server of WCP through a WAP network, the WML server will inform the cipher server to be responsible for actuating a public key remained in the handset software encryption and decryption module and the key management through the cipher server for the inter-process communication interface provided by operation systems of various computers; the public key is downloaded to the client, such as a mobile phone or a personal digital assistant, using HTTP service through a WAP gateway of WAN (wide area network), GSM/ GPRS/ CDMA and other digital mobile system.

3. The end to end real-time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1, wherein when it is

desired to down-link a personal commercial information, a user inputs a private key to be left in the stack memory of the mobile WAE environment as a standby key, when the WML server transfers the personal commercial information to be down-linked to the cipher server and inform the cipher server to open the public key remained in the handset software encryption and decryption module and key management for executing an encryption algorithm in the server end in advance; then, the handset software encryption and decryption module and the encrypted data are down-linked to a client through the HTTP service; then, the private key remained in the WAE executing environment is used to decrypt the encryption data and then the decryption plain text is transferred to display the original form through a WML format document for performing the following process.

4. The end to end real-time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1, wherein when it is desired to down-link a personal commercial information, the user inputs a private key to be left in a stack memory in the mobile WAE environment as a standby; when the WML server transfers the personal commercial information to be down-linked to the cipher server and inform the cipher server to open the public key remained in the handset software encryption and decryption module and key management for executing an encryption algorithm in the server end in advance; then, the handset software encryption and decryption module and the encrypted data are down-linked to the client through the HTTP service; then, the private key remained in the WAE executing environment is

used to decrypt the encryption data and then the decryption plain text is transferred to be displayed with the original form through a WML format document.

5. The end to end real-time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1, wherein responsibilities of the key management includes

a)key generation and conditions

an ideal key is generated randomly, unpredictable, and is kept in secret; furthermore, for the keys very demanded and updated frequently are generated by a pseudo random process; and

b) sharing the keys:

other than providing privacy and secret of the files and data through encryption technologies, a computer system used must assure that the encryption data can be restored; the key management has the mechanism of secret sharing, in that a key is divided into several key shadows; the original key is restored if only several key shadows of a specific number are combined; when the key is lost or destroyed, the data encrypted through this key can not be restored.

6. The end to end real-time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1, wherein a pre-compressor serves to compressor transmission data; a compressing procedure of the pre-compressor is:

a) dividing original data into several unit character string, and each character string has 8 or 9 characters;

b) converting each unit character string into a decimal value;

c) converting each decimal value into a unit character string of hexadecimal system;

d) dividing each unit character string of hexadecimal system into two unit character sets;

e) converting each unit character set into a decimal character code between 0 ~ 255; and

f) converting each character code directly into a respective ANSI character set;

In the aforesaid step a), to use 8 or 9 characters as an unit is based on the fact that the maximum data length supported by a mobile phone WAE executing environment is 64 bits, if the data is represented by a decimal system, it has a length of 10; therefore, in order to avoid data from overflowing, 8 or 9 characters are used as an unit.

7. The end to end real-time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1, wherein in the security mechanism, the handset software encryption and decryption module is based on the WAE application layer, and thus it is used to interpret wireless markup language, and wireless markup script language.